International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2s) 2026 pp. 1079-1099
https://doi.org/10.70917/ijcisim-2026-2190
Article

A SECURE BLOCKCHAIN-ASSISTED IOT FRAMEWORK FOR SMART AGRICULTURE USING QUANTUM-RESISTANT KEY VERIFICATION ALGORITHM (QRKVA)

K. Vaishnavi[1]*, Sumathy Kingslin[2]

[1]* PG & Research Department of Computer Science, Quaid-E-Millath Government College for Women (A), Chennai -600002, Tamil Nadu, India, vaishuangel25.7@gmail.com
[2]PG & Research Department of Computer Science, Quaid-E-Millath Government College for Women (A), Chennai -600002, Tamil Nadu, India
Corresponding Author: K. Vaishnavi (Email: vaishuangel25.7@gmail.com)

Abstract: Smart agriculture is an innovative approach to farming that incorporates IoT devices, blockchain technology, and AI security solutions to allow for real-time monitoring of produces, secure data management, intelligent decision-making, and efficient resource usage. However, with the increasing distribution of data from interconnected devices in agriculture derives significant threats to data privacy, secure communication, unauthorized access, data integrity and cyber threats. To address these challenges, a secure and privacy-preserving blockchain-based system is proposed, in which data collection is enabled by IoT devices on an agricultural farm to achieve enhanced data quality and efficient communication. Moreover, the Hash Based Block Creation Algorithm (HBCA) is used to create the blocks of the blockchain, which includes the agricultural data, time stamp, block ID, and the previous hash value. Following this, the Agricultural information is encrypted using the Blockchain based Advanced Encryption Standard-256 Secure Algorithm (BAES-256SA) which provides highly secured transmission and storage of agricultural information in the blockchain environment. Likewise, a Privacy-Aware Cryptographic Key Generation Algorithm (PA-CKGA) is presented to obtain secure encryption keys to safeguard sensitive data. In addition, Randomized Data Shuffling Algorithm (RDSA) improves security by shuffling the data generated by IoTs before stored in the blockchain or transmitted. Lastly, the Quantum-Resistant Key Verification Algorithm (QRKVA) confirms cryptographic keys, allowing for secure data access and decryption, and resists cyber and quantum computing attacks. The experimental outcomes reveal that the proposed framework is capable of providing secure, privacy-preserving, and reliable smart agriculture data management with the authentication success rate of 95.16%, which shows the effectiveness of the suggested framework..

Keywords: Smart Agriculture, Internet of Things (IoT), Blockchain, Data Security, Privacy Preservation, Hash-Based Block Creation Algorithm (HBCA), AES-256 Encryption, Cryptographic Key Generation, Data Shuffling, Quantum-Resistant Security, Secure Data Management

1. INTRODUCTION

With the development of the Internet of Things (IoT), blockchain, and artificial intelligence technologies, smart agriculture has revolutionized traditional farming into a smart and data-driven agricultural ecosystem. The smart agriculture systems involve the integration of various interconnected sensors, drones, smart irrigation systems, environmental monitoring systems, and automated agricultural machinery that gather real-time data from various aspects of agriculture, including soil moisture level, crop health, temperature, humidity, and water quality. These

technologies enhance agricultural productivity, ensure efficient resource use, lower operational costs, and contribute to sustainable farming. The massive scale rollout of IoT devices in agricultural settings, however, has also posed considerable security and privacy concerns because of the ongoing sharing of sensitive information across distributed networks.

Data insecurity is one of the significant challenges in smart agriculture due to the weak authentication mechanisms, insecure communication channels, limited computational power of IoT devices, and susceptibility to cyber threats like data tampering, spoofing, malware injection, denial of service attack, and unauthorized access. In general, agricultural IoT networks are deployed in open and remote settings where devices are extremely vulnerable to external threats. An attacker could alter sensor data, steal communication packets or take control of agricultural systems resulting in lost profits, decreased crop output, and loss of privacy for farmers [1]. Moreover, centralized data storage systems can also make the system vulnerable to single point failures and massive data leaks. Recent studies have highlighted the importance of blockchain technology in enhancing security and trust in IoT-enabled smart farming systems. By offering decentralized data management, immutability, transparency, and tamper-resistant communication, Blockchain mitigates the vulnerabilities of centralized data and communication systems. An IoT smart farm security framework based on the blockchain technology for enhancing secure data sharing, access control and device authentication in an IoT agricultural network [2]. Their solution provides a framework for the efficient protection of agricultural data from unauthorised tamper and possible hacking attempts.

Secure authentication and privacy-preserving communication are no longer optional features in today's smart farming solutions, alongside blockchain integration. To design a secure authentication protocol for IoT based smart farm monitoring system which is provably secure and can withstand replay attack, impersonation attack and ensures user anonymity. The study highlights the importance of using secure communication to ensure the confidentiality and integrity of data transfer between agricultural devices, and users [3]. One of the major challenges is privacy preservation, as smart agriculture systems continuously gather sensitive data concerning farm operations, production statistics, environment conditions, and user activities. Unauthorized disclosure of such information may lead to economic exploitation and privacy violations. A model for anomaly detection in agriculture that is privacy preserving and uses the IoTs to identify malicious activities while keeping the user and device data confidential [4]. Their work highlights the need for integrating intelligent anomaly detection and secure agricultural monitoring systems that take privacy concerns into account.

Furthermore, sophisticated cyber-attacks and the potential threat of quantum computing demand more robust security architectures of IoT ecosystems. An AI-based architecture that combines quantum-resistant blockchain mechanisms to maintain long-term security and privacy in IoT applications [5]. The framework integrates artificial intelligence, blockchain, and post-quantum cryptographic methods to deliver dynamic threat intelligence, communication security, and robust data protection, all designed to withstand the latest cyber threats. These methods are becoming more and more significant for future smart agriculture infrastructures, which heavily depend on interconnected intelligent devices. Therefore, ensuring data security, privacy preservation, secure authentication, and reliable communication has become a fundamental requirement in blockchain-enabled IoT smart agriculture systems. By incorporating blockchain, AI-powered security frameworks, privacy-enhancing features, and secure authentication systems, smart farms can enhance the trustworthiness and resilience of their environments against contemporary cyber threats.

Current smart agriculture security frameworks provide data protection and secure communication with the help of blockchain and IoT technologies, but there are still problems in many systems such as high computation cost, scalability, energy consumption, etc. and delay in real-time processing. Existing authentication and privacy-preserving systems have limited capabilities to defend against sophisticated cyberattacks and evolving threats in a large-scale agricultural setting. Furthermore, previous methods primarily address security aspects of a single security component, failing to provide a unified security framework that integrates AI-based threat detection, lightweight blockchain security, secure authentication and privacy protection. In this case, an efficient, scalable, and intelligent security framework is necessary to reliably and securely communicate on smart agriculture systems based on the IoTs.

1.1 Motivation of the research

Blockchain-assisted IoT smart agriculture systems are examined for Replay Attacks, Man-in-the-Middle (MITM) Attacks, Data Tampering Attacks, Unauthorized Access Attacks, and Quantum Computing Attacks by creating a comprehensive threat model.

As more smart agriculture equipment is being used, there is a huge amount of critical agricultural information being collected and must be handled securely.

Conventional security measures would not be adequate to safeguard data for agriculture against cyberattacks, access by unauthorized parties, and data tampering.

When IoT systems lack adequate integration with blockchain, it can create data integrity challenges and provide opportunities for misuse and lack of trust.

In distributed ag environments, current encryption solutions will not provide complete end-to-end security.

Key management in agricultural networks based on IoT is still a tough challenge to secure and efficient.

IoT data sent from devices is often consistent and can be easily hacked and attacked using patterns.

Farmers and agricultural systems require accurate, dependable, and tamper resistant data in real time to make informed decisions for improved productivity.

A comprehensive solution integrating blockchain, encryption, key management, and sophisticated security protocols is required to ensure strong protection.

The primary contribution of this research is the design and development of a secure and multi-layered blockchain-based IoT framework to provide high data privacy, integrity, and authentication in resource-limited and cyber-attack-prone smart agriculture environments. The proposed system combines real-time agricultural data collection using IoT with blockchain-based data immutability through HBCA and confidentiality using AES-256-based encryption. Furthermore, a PA-CKGA is added to create secure and dynamic encryption key, and a RDSA is used to enhance data security by increasing unpredictability before data stored and transmitted. Finally, the framework integrates a QRKVA to assure secure authentication and access control that are strong against even possible quantum computing attacks. This paper presents a comprehensive and future-proof security framework that enhances data security, communication efficiency, and trust in smart agriculture systems.

2. LITERATURE SURVEY

In this article [6], all studies on IoT-SF applications, privacy and security, communication and network layers, and sensors and devices were attempted to be integrated. Additionally, this study also examines the threats to security of IoT devices used in farming. This paper [7] presents the architecture and rationale of a smart IoT-based ecosystem for agricultural services. In addition, analyzed the potential and development trends of the IoT in precision agriculture and summarized the issues of IoT, particularly in agriculture. This research [8] presented a blockchain system for smart farming enabled by quantum-secure AI. A novel post-quantum cryptography (PQC) method based on Crystals-Dilithium is used in the strategy to protect against quantum attacks.

2.1 IoT security methods

Data processing, storage, and transmission are all made safe using the Elliptic Curve Cryptography (ECC) paradigm described in this paper. The ToN_IoT dataset was used to evaluate the proposed model, and the results demonstrate significant performance improvements, including fewer encryption and decryption operations [9].

In this paper, a new homomorphic signature scheme based on Hyperelliptic Curve (HEC) cryptography is proposed [10]. The signature encryption based on HEC reduces computational complexity and communication overhead, and enhances security compared with existing schemes.

This research introduced a new blockchain-based smart agricultural IoT system architecture that uses trusted data to control the agricultural production environment [11]. Furthermore, this system secures identities and ensures traceability of data and devices by combining Elliptic Curve Integrated Encryption (ECIES) with group signatures.

The Cybersecurity Framework for Efficient Agriculture (CSFSA) is developed on the Constrained Application Protocol (CoAP). The CSFSA is proposed to provide secure, reliable authentication for IoT devices, ensuring data authenticity and integrity [12].

In this research [13], a foundational protocol for an ECC-based smart agricultural monitoring system was proposed, offering efficiency and privacy protection. The suggested ECC architecture can provide secure communication in effective agricultural monitoring systems and overcome a variety of security threats.

An IoT-based random forest model for smart farming to enhance crop production is presented [14]. In addition, an AI-based precision model is implemented in the system, which can be coupled with remote sensor data to enable accurate prediction of crop growth in smart agriculture. However, energy and labor account for about 40% of the greenhouse's production costs.

This paper proposes a consensus framework for the early detection of agricultural theft that employs decentralised storage to secure data, Digital Signature Algorithms (DSA), and ECC as security features. The current state of the art employs deep learning models and blockchain-based architectures to predict agricultural yields for efficient, robust agriculture. However, the two mentioned are less commonly combined to suggest a full framework for working efficiently in agriculture [15].

2.2 Blockchain security

A novel hybrid Recurrent Neural Elliptical Curve Blockchain (RNECB) was proposed in [16] to securely store sensed agricultural data. This method's monitoring mechanism offers continuous monitoring and the extraction of significant characteristics.

To enhance the security system [17], design a Decentralized Blockchain Provenance Security System (DBPSS) to ensure trustworthy data security for agricultural information distribution in a distributed network. Next, the security validates the individual block-key codes within each transaction via provable availability to aid verification in a distributed environment.

To enhance the security of IoT-based smart irrigation systems, this research [18] presented a security architecture based on ECC and Secure Hash Algorithm 256 (SHA-256). However, a variety of attackers, including "white-hat" hackers who seek to test the system's exploitable capabilities, often target IoT infrastructure.

Identifying characteristics for each link of the agricultural supply chain, designing, evaluating, and implementing strategies, and deploying them as smart contracts on the blockchain platform is a multi-step process for developing a traceable Attribute-Based Access Control (ABAC) scheme [19].

The novel [20] proposed a multi-layer blockchain system for agricultural data management, which can accurately track aspects such as supply chain monitoring, land management, market transactions, and sustainability monitoring.

Table 1. Secure Privacy Preserving based on Smart Agriculture

Author	**Year**	**Classification Technique**	**Limitation**	**Performance Metrics**
Kee S.N [21]	2024	AES-256	Limited scalability analysis and high computational cost	Authentication Accuracy, Security Strength
Kalimuthu [22]	2024	Capsule Neural Network (CapsNet),	Increased encryption complexity	Accuracy, Encryption Time
Zhang [23]	2022	Ciphertext-Policy Attribute-Based Encryption (CP-ABE) algorithm	High computational cost	Security Level, Communication Overhead
Kiran [24]	2023	Evolutionary Adaptive Swarm Intelligent Sparrow Search (EASISS)	Cluster formation overhead affects network efficiency in dense IoT networks	Energy Consumption, Network Lifetime,
Bhandiwad [25]	2025	Advanced Elgamal signature (AES)	Lightweight encryption may reduce robustness against advanced attacks	Computational Cost, Security Efficiency

Zhang, G [26]	2021	Re-Encryption based on Ciphertext-Policy Attribute Encryption (RE-CP-ABE)	Complex attribute management and increased storage overhead	Privacy Preservation Rate
Shaik [27]	2024	Attention Bidirectional Gated unit assisted Residual network (Att-BGR)	computational resources	F1-Score, Secure Transmission Rate
Vedula [28]	2026	Optimal multi-key based Fully Homomorphic Encryption (OMK-FHE)	Ethereum integration introduces transaction latency	Pest Detection Accuracy, Irrigation Efficiency

Table 1 details the classification methods' performance variables and limitations from the prior dataset, which are used to deliver secure privacy protection for intelligent agriculture.

The paper recommends methods to increase field crop yields through pest and disease control, an essential part of national economic development. These outcomes, together with a 93.61% accuracy rate, demonstrate the approach's effectiveness in smart agriculture and its ability to enhance monitoring and security of smart agriculture systems using blockchain. By applying Secure ECC (SECC) and advanced multi-user authentication and key-generation techniques, this work [30] introduced an efficient and secure agriculture environment to secure smart agriculture systems.

2.3 Problem Statement

IoT devices are crucial to smart agriculture systems as they enable real-time data collection and monitoring.

Agricultural data generated by IoT devices is extremely susceptible to cyber-attacks, unauthorised access and data breaches.

In distributed IoT agricultural environments, the traditional security solutions are not enough to achieve end-to-end security.

The dynamic and secure management of cryptographic keys is still a big challenge in present smart agriculture frameworks.

There is lack of advanced features like data randomization or obfuscation in most of the existing systems, which make them susceptible to the pattern-based attacks.

As quantum computers pose threats, current encryption methods might not work in the future.

There is a lack of a unified, scalable, and efficient framework that integrates IoT, blockchain, encryption, and quantum-resistant security.

2.4 Objective of the research

To develop secure smart agriculture system for real-time data collection and monitoring using IoT.

To apply the concept of blockchain for agriculture data integrity, transparency and no-tamper storage of agricultural data.

To improve data privacy with the use of advanced encryption methods like AES-256 for secure data transfer and storage.

To design a secure and dynamic PA-CKGA for key management.

To enhance the security of data by employing a RDSA to obfuscate data generated by IoT devices before it is stored or transmitted.

To develop a HBCA to create an efficient and secure block formation in blockchain.

To present a QRKVA to create a secure authentication system and resist quantum computing attacks.

To proposed framework for its security, accuracy and efficiency of data protection in smart agriculture systems

3. PROPOSED METHODOLOGY

In this section, the proposed blockchain-based IoT framework for smart agriculture is presented. The framework combines secure block creation, data encryption, generation of cryptographic keys, shuffling of data, and quantum-resistant key verification to ensure secure, privacy-preserving, and reliable management of agricultural data.

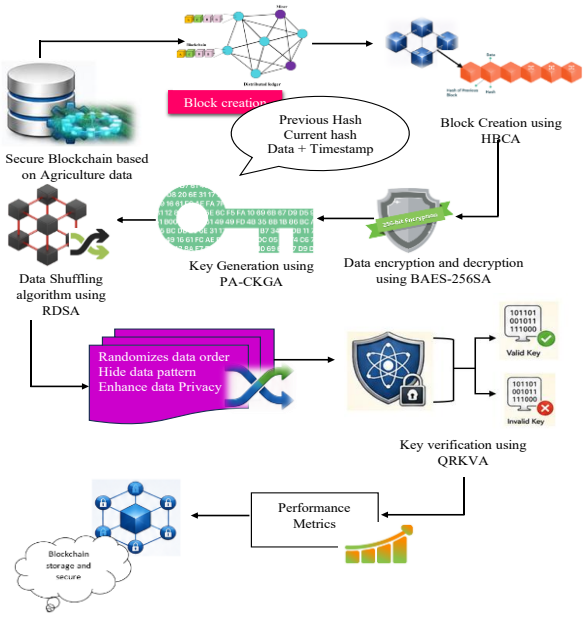

Figure 1. Proposed Method Based on Architecture Diagram

The overall architecture of the proposed blockchain-assisted IoT framework for smart agriculture using the QRKVA is shown in figure 1. Agricultural data are gathered from different IoT-enabled devices placed at the farm, such as soil moisture sensors, temperature sensors, humidity sensors, pH sensors and weather monitoring systems. The processed data is then sent to the HBCA where they are used to generate secure blockchain blocks which includes the agricultural data, blockchain block identifiers, timestamps and previous hash values. Then, the PA-CKGA produces robust cryptographic keys derived from the privacy and security parameters. The BAES-256SA uses these keys for data encryption, secure data transmission and storage of agricultural information. To ensure further security, the RDSA scrambles the data to be stored in a blockchain, so as to make it hard for the attacker to make any pattern-based attacks and it is also impossible to analyze the data without the permission of the RDSA. The encrypted data is stored and transmitted securely and tamper-proofly through the blockchain network after shuffling. When data is accessed, the QRKVA checks the authenticity of cryptographic keys and users, and only allows access to the data once the checks have been completed. Lastly, authorized users can access and utilize agricultural data securely for monitoring crops, managing irrigation, predicting diseases, and making intelligent farming decisions.

3.1 Threat Model

The proposed blockchain assisted IoT smart agriculture framework is a distributed system that includes the IoT sensor, the blockchain nodes, communication networks and authorized users. Since agricultural deployments are public, the system is vulnerable to a variety of attacks, which may compromise the confidentiality, integrity, authenticity and availability of data. Furthermore, a threat model is proposed to analyze the security strength of the proposed QRKVA framework.

Replay Attack

Valid communication packets may be captured by an attacker and retransmitted to increase unauthorized access or disrupt agricultural operation. The proposed framework resolves replay attacks by using the timestamp-based validation, unique block identifier, and dynamically generated cryptographic key by PA-CKGA.

Man-in-the-Middle (MITM) Attack

Data can be hacked and altered during the interaction between the IoT devices and the blockchain nodes. Secure communication and prevention of unauthorized editing of agricultural information is achieved through the implemented BAES-256SA encryption mechanism and QRKVA key verification.

Data Tampering Attack

A hacker could try to change farming data stored on the blockchain. The HBCA module is capable of creating cryptographic hashes and connecting blocks using chained hash values, allowing for easy detection of unauthorized alterations and ensuring data integrity.

Unauthorized Access Attack

Confidential agricultural information may be accessed by unauthorized users. The PA-CKGA and QRKVA modules implement secure key generation, authentication and verification processes to allow only valid users to gain access to the encrypted data.

Quantum Computing Attack

Quantum algorithm can break classic cryptographic methods like RSA, ECC, and other algorithms. To overcome this challenge, the proposed QRKVA framework uses the Dilithium -Kyber post quantum cryptographic mechanism to generate and verify the keys. Since Kyber is based on lattice cryptography and the hardness of the MLWE problem, the framework provides strong resistance against both classical and quantum adversaries.

In the field of smart agriculture, the combination of HBCA, BAES-256SA, PA-CKGA, RDSA, and QRKVA forms a multi-layer security framework, providing protection against replay attacks, man-in-the-middle attacks, data tampering, unauthorized access, and quantum threats.

3.2 Hash-Based Block Creation Algorithm (HBCA)

The HBCA is used to create safe blocks in the blockchain using the information from agricultural devices on the IoT. First, the agricultural information measured, for example, soil moisture, soil temperature, soil humidity and various crop parameters are collected and stored in a structured data format. Then, a unique block is created by storing the agricultural data on the blockchain with some essential attributes of the blockchain such as a time stamp, a unique block identifier (Block ID) and the hash of the previous block. These elements together make up the block content, which guarantees the distinct identification of each block and its chronological association with the preceding block content. Once the block info is compiled, a cryptographic hash function is calculated to create a unique current hash value that represents the content of the entire block. This hash value acts as a digital fingerprint of the block, allowing it to be checked for any unauthorized changes. The resulting current hash is added to the blockchain and serves as the previous hash value for the next block in the chain to be created. The chained hashing mechanism provides the HBCA with an unchangeable and tamper-proof blockchain structure, which ensures that agricultural information in the smart agriculture system is stored securely and managed reliably, while also ensuring the integrity, authenticity, and traceability of agricultural information.

As indicated in the equation 1, compute the blockchain block, which consists of agricultural data, timestamp, block ID, and previous block hash. Let's assume $B_i -$ current block, $D_i -$ agricultural data $T_i -$ timestamp, $ID_i -$unique block identifier, $H_{i-1} -$hash value of the previous block.

$$B_i = (D_i, T_i, ID_i, H_{i-1}) \quad (1)$$

As illustrated in equation 2, creates a unique cryptographic hash of the present block for data integrity and resistance to tampering. Let's assume $H_i -$current block hash, $Hash(\cdot) -$ cryptographic hash function, $B_i -$current block content.

$$H_i = Hash(B_i) \quad (2)$$

According to equation 3, calculate the connection of the two adjacent blocks of the blockchain by using chained hash values. Let's assume $L_i -$blockchain linkage, $H_{i-1} -$previous block hash, $B_i -$current block, $H_i -$current block hash.

$$L_i = H_{i-1} \rightarrow B_i \rightarrow H_i. \quad (3)$$

As indicated in equation 4, verifies if the content of the blocks stored has not changed by comparing the recalculated hash with the stored hash value. Let's assume I_i −integrity status, 1– valid block; 0– tampered block, $Hash(B_i)$ −recalculated hash, H_i − stored hash value.

$$I_i = \begin{cases} 1, & Hash(B_i) = H_i \\ 0, & otherwise \end{cases} \quad (4)$$

By combining agriculture information, timestamp, block ID and previous hash value, HBCA successfully creates a secure blockchain block and then generates the cryptographic hash. This process guarantees the integrity, immutability, traceability and tamper resistant storage of agricultural information in the blockchain network.

3.3 Blockchain-based AES-256 Secure Algorithm (BAES-256SA)

The BAES-256SA is used for encrypting agricultural information prior to its transmission or storage in the blockchain environment. Furthermore, the agricultural data preparation is to make sure the data gathered from the farming devices is suitable and in an appropriate format for encryption. After that the agricultural data is scrambled with a cryptographic key produced by the key management module, which is 256 bits in size. The AES-256 encryption process takes plaintext data, applies a series of substitution, permutation, and transformation operations, and finally adds encryption keys to the data to create the resulting ciphertext. This encrypted data is then safely stored in the blocks of the blockchain or sent through the network, making sure that no one can access delicate agricultural data without authorization. The original agricultural data can be retrieved by the AES-256 decryption during data retrieval by the authorized user who has the valid decryption key. By combining blockchain technology with AES-256 encryption, the BAES-256SA ensures confidentiality, secure communication, data privacy, and protection against unauthorized access, thereby enhancing the overall security of smart agriculture systems.

Before storing the agricultural information in the blockchain, it is encrypted by the secret key and initialization vector of AES-256 as illustrated in equation 5. Let's assume D_i– agricultural data packet, K_i– 256-bit encryption key, IV_i– initialization vector, C_i– encrypted ciphertext, AES_{256}– AES-256 encryption function.

$$C_i = AES_{256}(D_i, K_i, IV_i) \quad (5)$$

Applies multiple rounds of iterative AES transformations to improve data confidentiality, as shown in equation 6. Let's assume$S_i^{(r)}$– state matrix at round r, $S_i^{(r-1)}$– previous round state matrix; $SB(\cdot)$– SubBytes transformation, $SR(\cdot)$– ShiftRows transformation, MC– Mix Columns transformation, $RK_i^{(r)}$– round key for round r, $\oplus$– XOR operation.

$$S_i^{(r)} = MC\left(SR\left(SB\left(S_i^{(r-1)}\right)\right)\right) \oplus RK_i^{(r)} \quad (6)$$

Generates round specific cryptographic keys from the original 256-bit secret key, as illustrated in equation 7. Let's assume$RK_i^{(r)}$– round key, K_i– master secret key, r– encryption round index, $KeySchedule(\cdot)$– AES key expansion function.

$$RK_i^{(r)} = KeySchedule(K_i, r) \quad (7)$$

As presented in equation 8, creates a blockchain block with encoded agricultural information and security metadata. Let's assumeB_i– blockchain block, ID_i– block identifier, T_i– timestamp, C_i– encrypted data, H_{i-1}– previous block hash, N_i– nonce value

$$B_i = \{ID_i, T_i, C_i, H_{i-1}, N_i\} \quad (8)$$

Generates a hash of the blockchain to signify block integrity and tamper-resistant, as presented in equation 9. Let's assume H_i– current block hash, $SHA256(\cdot)$– cryptographic hash function, ‖– concatenation operator, N_i– random value.

$$H_i = SHA256(ID_i \| T_i \| C_i \| H_{i-1} \| N_i) \quad (9)$$

Calculate the newly created encrypted block and add it to the blockchain ledger, as indicated in equation 10. Let's assumeBS_i– blockchain storage ledger, B_i– current block, B_{i-1}– previous blockchain state, H_i– current block hash, ∪– union operation.

$$BS_i = B_{i-1} \cup \{B_i, H_i\} \tag{10}$$

Recovers the original agricultural information from encrypted blockchain data, as shown in equation 11. Let's assume$\widehat{D}_i$– recovered agricultural data, C_i– ciphertext, K_i– secret key, IV_i– initialization vector, $AES_{256}^{-1}(\cdot)$– AES decryption function.

$$\widehat{D}_i = AES_{256}^{-1}(C_i, K_i, IV_i) \tag{11}$$

The BAES-256SA method is an encrypted agricultural data repository secured by blockchain technology which allows for secure storage and exchange of agricultural information.

3.4 Privacy-Aware Cryptographic Key Generation Algorithm (PA-CKGA)

The PA-CKGA is proposed to ensure the security of cryptographic keys needed to safeguard sensitive agricultural information in the smart agriculture framework based on the blockchain. Moreover, attributes of privacy, user credentials, device information and security parameters are gathered and processed to create an environment of secure key generation. These parameters are then added together and processed using cryptographic functions to create a unique encryption key that has high randomness and unpredictability. A key is generated and securely linked to the agricultural data and used by the encryption module to protect confidential information when storing and transmitting the data. In addition, the algorithm is designed to continuously meet the requirements of privacy and security, which helps to prevent unauthorized access and minimizes the possibility of attacks based on keys. PA-CKGA creates robust and private cryptographic keys, which boosts the security of the smart agriculture system, bolsters access control systems, and contributes to the overall data security of the smart agriculture system.

Comprehends privacy related data of the user, devices and security parameters for key generation, as given in equation 12. Let's assume P_i– privacy parameter vector; U_i– user credentials; D_i– device information; S_i– security attributes; $\omega_1, \omega_2, \omega_3$– weighting coefficients.

$$P_i = \omega_1 U_i + \omega_2 D_i + \omega_3 S_i \tag{12}$$

Generates a random cryptographic seed with privacy parameters and dynamic security parameters, as indicated in equation 13. Let's assume R_i– random seed value, P_i– privacy parameter vector, T_i– timestamp, N_i– random value, $Hash(\cdot)$– cryptographic hash function, ‖– concatenation operator.

$$R_i = Hash(P_i \| T_i \| N_i) \tag{13}$$

Generates a unique cryptographic encryption key based on the generated random seed and privacy information, as shown in equation 14. Let's assume K_i– generated encryption key, R_i– random seed, P_i– privacy parameters, ID_i– user/device identifier.

$$K_i = Hash(R_i \| P_i \| ID_i) \tag{14}$$

Calculate the randomness and strength of the cryptographic key generated, as shown in equation 15. Let's assume KS_i– key strength score, $Entropy(K_i)$– entropy of generated key, L_i– key length.

$$KS_i = \frac{Entropy(K_i)}{L_i} \tag{15}$$

Validates the generated key meets the required privacy and security level, as shown in equation 16. Let's assume V_i– validation status, KS_i– key strength, θ– security threshold, 1– valid key, 0– invalid key.

$$V_i = \begin{cases} 1, & KS_i \geq \theta \\ 0, & KS_i < \theta \end{cases} \tag{16}$$

The PA-CKGA produces a robust and privacy-preserving cryptographic key to provide secure data encryption, access control, and safeguarding of sensitive agricultural data in storage and during transmission.

3.5 Randomized Data Shuffling Algorithm (RDSA)

The RDSA method is presented to secure the encryption of agricultural data prior to blockchain storage or network transmission. The data sequence comprises the data generated by the agricultural devices, which are encrypted using the IoT device. Then a randomisation mechanism is used to create a new shuffling pattern depending on the security parameters and random values. With the pattern, the locations of the data elements are scrambled, but the data themselves remain the same. This shuffling process makes it hard for an attacker to detect meaningful patterns, or be able to glean sensitive information while transmitting or storing the data. The scrambled encrypted data are then passed over the blockchain network for secure storage and communication. In an authorized retrieval, the data sequence is restored to its original sequence prior to decryption, through the process of inverse shuffling. The integration of an extra layer of randomness boosts the data confidentiality, increases traffic analysis and pattern-based attack resistance, and increases overall smart agriculture security.

Before shuffling, compute the encrypted agricultural data sequence received from the IoT devices as illustrated in equation 17. Let's assume E −encrypted data sequence, C_i −encrypted data element, n– total number of encrypted records.

$$E = \{C_1, C_2, C_3, \dots, C_n\} \tag{17}$$

Generates a random permutation pattern, using security parameters and random values, as shown in equation 18. Let's assume P– shuffling permutation vector; $CSRNG(\cdot)$– cryptographically secure random number generator, S_i– security parameter, T_i– timestamp.

$$P = Rand\big(CSRNG(S_i, T_i, N_i)\big) \tag{18}$$

Rearranges encrypted elements in data based on the permutation pattern generated, as shown in equation 19. Let's assume SE_i– shuffled encrypted data, E– original encrypted sequence, P_i– permutation index at position i.

$$SE_i = E(P_i) \tag{19}$$

As illustrated in equation 20, Constructs is a function that creates a blockchain block with shuffled encrypted data and blockchain metadata. Let's assume B_i– blockchain block, ID_i– block identifier, T_i– timestamp, SE_i– shuffled encrypted data, H_{i-1}– previous block hash

$$B_i = \{ID_i, T_i, SE_i, H_{i-1}\} \tag{20}$$

Recovers the original encrypted data sequence by applying the inverse permutation, as in equation 21, when accessing the data in an authorized manner. Let's assume E_i– recovered encrypted data, SE– shuffled encrypted sequence, P_i^{-1}– inverse permutation index.

$$E_i = SE(P_i^{-1}) \tag{21}$$

Calculate the measure of randomness added to the data as a result of the shuffling process, as presented in equation 22. Let's assume SS– shuffling security score, P_i– shuffled position, i– original position, n– total number of data elements.

$$SS = \frac{\sum_{i=1}^{n} |P_i - i|}{n} \tag{22}$$

The RDSA creates a randomly shuffled encrypted dataset that hides the order of the data, thereby ensuring greater confidentiality and strengthening security before storing or transmitting the data on the blockchain.

3.6 Quantum-Resistant Key Verification Algorithm (QRKVA)

The QRKVA is a blockchain-based cryptographic security system that can be used to guarantee safe communications and protected access to data in smart agriculture environments. The algorithm works by creating a post-quantum cryptographic key and the authenticity of the key is confirmed using blockchain-based authentication and distributed validation. QRKVA verifies authorized user and IoT devices before granting access to the encrypted agricultural data during the communication process. Moreover, the QRKVA method provides secure key verification and integrity validation procedures to prevent cyber-attacks, unauthorized access, and quantum computing attacks to smart farming information. Therefore, QRKVA increases the data confidentiality, communication security and reliable access control in smart agriculture systems based on a blockchain.

The proposed QRKVA framework uses lattice-based key encapsulation mechanism, which is a NIST standardized post-quantum cryptographic algorithm, to enable practical security for the future. Instead of relying on the difficulty of the RSA or ECC problems like with classic public-key crypto schemes, Dilithium -Kyber is built on the Module Learning With Errors (MLWE) problem. The secret keys generated are based on Kyber and are used in the key verification process to provide secure communication channels and authenticated access control. Therefore, the proposed scheme is safe from classical cryptographic attacks and future attacks using quantum computers of large size.

Evaluate a secure Dilithium-Kyber post-quantum encryption key—capable of resisting quantum computing attacks and used for communication security, authentication, and access control—as shown in Equation 23 Let's assume K_{qr} − Quantum-resistant secret key, Gen − Key generation function, PQ_p − post-quantum parameters, R_n −Random nonce value, S_s − Security seed.

$$K_{qr} = Gen(PQ_p, R_n, S_s) \tag{23}$$

The Encrypts smart agriculture data is provided by employing a quantum-resistant cryptographic encryption method, as illustrated in equation 24. Let's assume C_t −Ciphertext data, Enc −Encryption function, D_{sf} −Smart farming data, K_{qr} −Quantum-resistant key.

$$C_t = Enc(D_{sf}, K_{qr}, IV) \tag{24}$$

Generates a blockchain hash on data that has been encrypted to ensure integrity and tamper-proof storage, as in equation 25. Let's assume H_b – Blockchain hash value, $SHA3\text{-}512$ – Secure hash function, C_t – Ciphertext, T_s – Timestamp, H_{b-1} – Previous block hash, ‖– Concatenation operator

$$H_b = SHA3\text{-}512(C_t \| T_s \| H_{b-1}) \tag{25}$$

As indicated in equation 26, validates access to authorized users and verifies authenticity of the cryptographic key using blockchain authentication. Let's assume V_{qr} – Verification status, $Verify$ – Verification function, K_{qr} – Quantum-resistant key, U_{id} – Authorized user identity, H_b – Blockchain hash value, 1– Successful verification.

$$V_{qr} = Verify(K_{qr}, U_{id}, H_b) = 1 \tag{26}$$

As described in Equation 27, decrypt the ciphertext with the verified quantum-resistant key to retrieve the original smart farming information securely. Let's assume D_{sf} −Recovered smart farming data, Dec −Decryption function, C_t −Ciphertext data, K_{qr} −Quantum-resistant secret key.

$$D_{sf} = Dec(C_t, K_{qr}, IV) \tag{27}$$

The proposed QRKVA framework is designed to securely safeguard smart agriculture data using blockchain technology features such as encryption, quantum-resistant key verification, authenticated access control, and privacy-preserving communication.

3.7 Security Analysis

The proposed QRKVA framework uses a multi-layer security architecture that comprises of HBCA, BAES-256SA, PA-CKGA, RDSA, and QRKVA to defend against different cyber threats in the smart agriculture systems. The following section discusses the security threats that can be faced by the suggested framework.

Resistance to Replay Attacks

In replay attacks, an attacker receives legitimate messages of the communication process and resends them to gain unauthorized access or to disrupt system operations. The suggested structure involves the use of timestamps, unique block identifiers, dynamically-generated cryptographic keys, and validation mechanisms for blockchain transactions. Each individual communication session has different parameters and timestamps, so previous messages will be invalid if they are retransmitted. Replay attacks are thus easily detected and prevented.

As shown in Equation 28, calculate the difference between the timestamps to accept the received message within the permissible limit.

$$V_{Replay} = \begin{cases} 1, & | T_{current} - T_{msg} | \leq \Delta T \\ 0, & otherwise \end{cases} \tag{28}$$

Where V_{Replay} − Replay attack validation status, $T_{current}$ − Current timestamp, T_{msg} − Received message timestamp, ΔT= Maximum allowable delay.

Resistance to Man-in-the-Middle (MITM) Attacks

The attacker intercepts, modifies or injects malicious information during the communication between IoT devices and blockchain nodes in a MITM attack. The BAES-256SA module encrypts all agricultural information before transmitting, and QRKVA can check the authenticity of the cryptographic key and the communicating entity. An attacker would not be able to change the transmitted data, because it would not be verified upon reception of the change.

Evaluate the authenticity of the encrypted message and the hash validation, as shown in Equation 30.

$$V_{MITM} = \begin{cases} 1, & H(C_{received}) = H(C_{stored}) \\ 0, & otherwise \end{cases} \quad (29)$$

Where $C_{received}$ −Received ciphertext, C_{stored} −Original ciphertext $H(.)$ − Cryptographic hash function

Resistance to Data Tampering Attacks

Data tampering attacks are aimed at changing agricultural information within the system. Each block in a blockchain has a hash value, which is generated by the HBCA module that is calculated based on the data in the block. The HBCA module creates a hash value for each block in the blockchain, and the hash value of each block is linked to the hash value of the previous block. The integrity of the blockchain is broken if any part of the stored data is changed, which changes the hash value and alerts everyone. This makes it easy to identify and refuse changes that are not authorized.

Verify the blockchain integrity by comparing the current and recalculated hashes, as shown in Equation 29.

$$I_{Block} = \begin{cases} 1, & Hash(B_i) = Hash'(B_i) \\ 0, & otherwise \end{cases} \quad (30)$$

Where I_{Block} −Block integrity status, $Hash(B_i)$ −Stored block hash, $Hash'(B_i)$ − Recalculated block hash.

Resistance to Unauthorized Access Attacks

Unauthorized users may try to get access to private agricultural data without proper access credentials. The PA-CKGA creates cryptographic keys that are privacy-preserving based on user credentials, device information, and security attributes. Additionally, QRKVA securely verifies keys before providing access privileges. Consequently, only legitimate users with appropriate cryptographic credentials will be able to access sensitive agricultural information.

Calculate the identity and key verification as shown in Equation 31.

$$A_{Access} = V_{User} \times V_{Key} \quad (31)$$

Where A_{Access} − Access authorization status, V_{User} − User authentication result, V_{Key} − QRKVA key verification result

Resistance to Pattern-Based Attacks

Pattern-based attacks try to deduce sensitive information from the way communications are made. The module RDSA proposed by our group scrambles the agricultural data to be stored or transmitted to other network nodes in a random sequence. This randomisation obscures the original sequence of data, and greatly diminishes the risk of information leakage via traffic analysis or pattern recognition.

Resistance to Quantum Computing Attacks

The proposed QRKVA framework covers quantum-resistant key generation and verification algorithm Dilithium-Kyber. The security of Kyber relies on the Module Learning With Errors (MLWE) problem, which is believed to be hard for classical and quantum computers to solve efficiently. As a result, even with the advent of large-scale Quantum computers, the proposed framework could maintain the secure authentication, key exchange, and ensure protected access to agricultural information.

The proposed QRKVA framework is designed to be highly effective in combating replay attacks, man-in-the-middle attacks, data tampering, unauthorized access, pattern-based attacks, and quantum computing threats, through

its integration of blockchain-based immutability, AES-256 encryption, privacy-aware key generation, randomized data shuffling, and quantum-resistant authentication. As a result, the framework guarantees safe, secure, and trustworthy agricultural data management in smart farming settings, where IoT devices are playing a crucial role.

4. RESULT AND DISCUSSION

The experimental results show that the proposed QRKVA approach secure and privacy-preserving ai-driven framework for smart agriculture using blockchain provides optimal security and IoT communication performance compared to existing smart agriculture systems. In addition, the proposed QRKVA scheme is compared with the advanced security schemes such as ECC, DSA, RNECB, and SHA-256. Experimental results showed that the proposed system has low encryption and decryption times, low system latency, high throughput, better authentication reliability, better secure communications reliability, low packet loss rate, and high overall system accuracy.

Table 2. Simulation Parameter

Parameter	**Value**
Network Type	IoT
Number of IoT Nodes	50 – 500 Nodes
Data Transmission Rate	250 kbps – 1 Mbps
Packet Size	64 Bytes / 128 Bytes
Simulation Area	1000 m × 1000 m
IoT Device Energy	5 Joules
Network Coverage Range	50 – 100 meters
Blockchain Block Size	1 MB
Cloud/Edge Support	Edge Computing Enabled
AI Training Epochs	50 – 100
Batch Size	32 / 64
Learning Rate	0.001

As shown in table 2, the simulation settings are the working settings of the proposed QRKVA secure AI-driven IoT smart agriculture framework. IoT sensor nodes are distributed in a 1000 m × 1000 m farmland to gather and send real-time farm information with a good communication rate and packet size. The system combines block chain security, edge computing service, and AI training options including epochs, batch size, and learning rate to provide accurate prediction, secure communication, and effective agriculture monitoring.

Table 3. Overall Performance of Comparison Metrics

Method	**Throughput (Mbps)**	**Authentication Reliability (%)**	**Secure Communication (%)**	**Packet Loss Rate (%)**	**System Latency (ms)**	**Encryption Time (ms)**	**Decryption Time (ms)**	**Accuracy (%)**
ECC	80.84	84.63	85.09	4.92	21.8	6.85	6.42	75.30
DSA	83.12	85.41	86.74	4.46	19.6	6.12	5.78	78.62
RNECB	84.63	87.55	88.62	4.11	17.4	5.46	5.21	82.47

SHA-256	86.76	89.38	89.85	3.87	14.2	4.83	4.57	87.18
QRKVA	89.94	93.24	94.12	2.38	8.9	3.21	2.94	95.16

According to the results in the table 3, the proposed QRKVA framework for smart farming using Blockchain-AES-128 and QRKVA technology shows significantly higher results compared to ECC, DSA, RNECB and SHA-256 for throughput (89.94 Mbps), authentication dependability (93.24%), secure communications (94.12%), and accuracy (95.16%), as well as the lowest packet loss rate (2.38%), system latency (8.9 ms), encryption time (3.21 ms), and decryption time (2.94 ms).

Table 4. Attack Resistance Comparison of Existing Methods and Proposed QRKVA Framework

Attack Type	**ECC (%)**	**DSA (%)**	**RNECB (%)**	**SHA-256 (%)**	**QRKVA (%)**
Replay Attack Resistance	79.42	82.16	85.37	88.54	93.24
MITM Attack Resistance	80.15	83.42	86.28	89.36	93.78
Data Tampering Resistance	81.36	84.75	87.92	90.41	94.00
Unauthorized Access Resistance	79.84	82.93	86.17	89.58	93.62
Pattern-Based Attack Resistance	79.26	81.54	84.83	88.16	92.74
Quantum Attack Resistance	79.00	80.35	82.64	85.27	93.15
Overall Attack Resistance	79.84	82.53	85.54	88.55	93.42

Table 4 shows the comparison result of attack-resistance among the proposed QRKVA scheme and other existing schemes. The proposed QRKVA protocol provides better protection against replay, MITM, data manipulation, unauthorized access, pattern and quantum attacks with attack-resistance ranging from 92.74 % to 94.00%. The enhanced performance due to combined influence of Blockchain integrity verification, BAES-256SA encryption, privacy-aware key generation, randomized data shuffling, and quantum-resistant key verification techniques. These results validate the effectiveness of our pro- posed framework in securing IoT-based smart agriculture environment against potential threats.

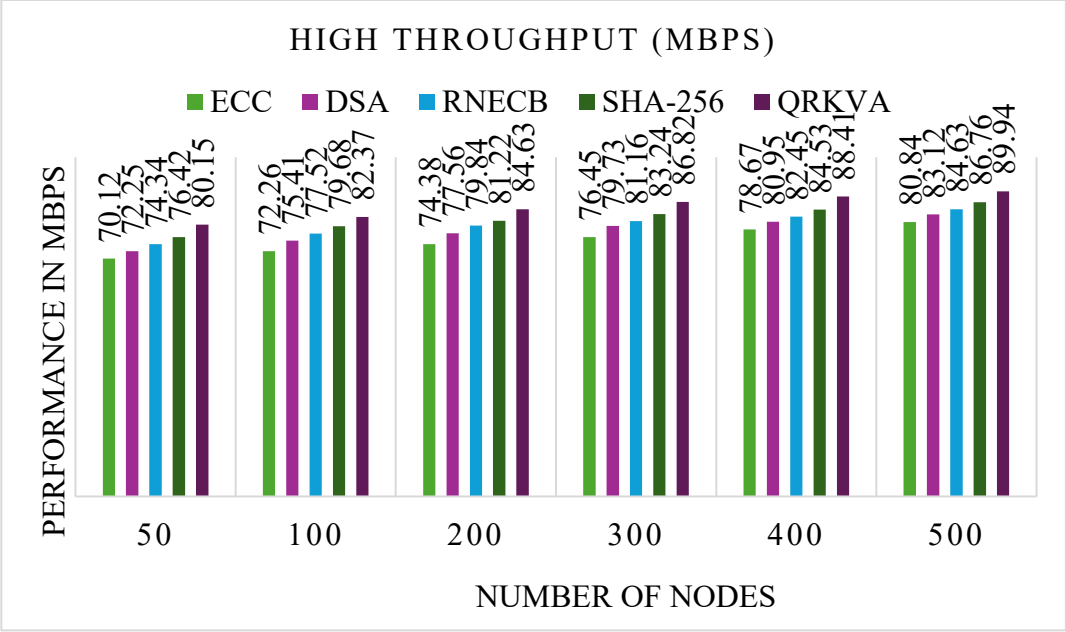

Figure 2. Analysis of High Throughput (Mbps)

As shown in Figure 2, a comparison was made between existing methods in smart farming systems and the proposed QRKVA smart agriculture using a blockchain technique. Moreover, the efficiency analysis shows that the QRKVA technique achieves a throughput of 89.94 Mbps compared with other methods. Moreover, in comparing the QRKVA technique with respect to other methods ECC, DSA, RNECB, and SHA-256, the corresponding throughput rates during the efficiency analysis are 80.84 Mbps, 83.12 Mbps, 84.63 Mbps, and 86.76 Mbps, respectively.

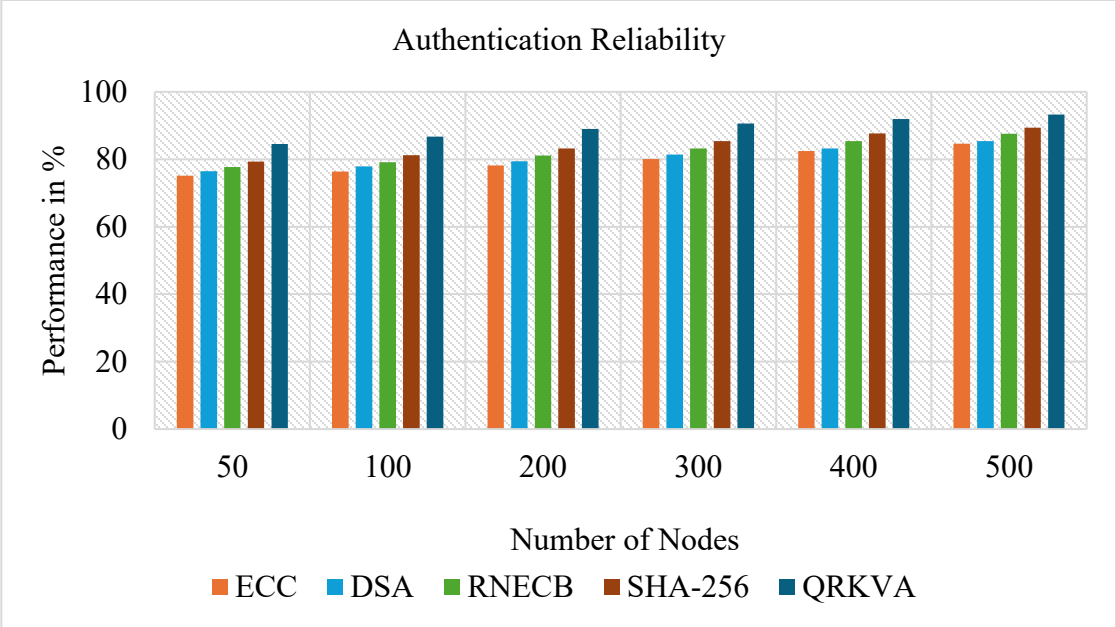

Figure 3. Analysis of Better Authentication Reliability

As illustrated in Figure 3, the comparison was conducted among existing techniques for smart farming systems and the QRKVA blockchain-based smart agriculture. Furthermore, the performance analysis indicates that the QRKVA method achieves a superior authentication reliability of 93.24% compared with other methods. In addition, when the QRKVA scheme is compared with the existing schemes ECC, DSA, RNECB, and SHA-256, the Better Authentication Reliability rates are 84.63%, 85.41%, 87.55%, and 89.38%, respectively, during performance analysis.

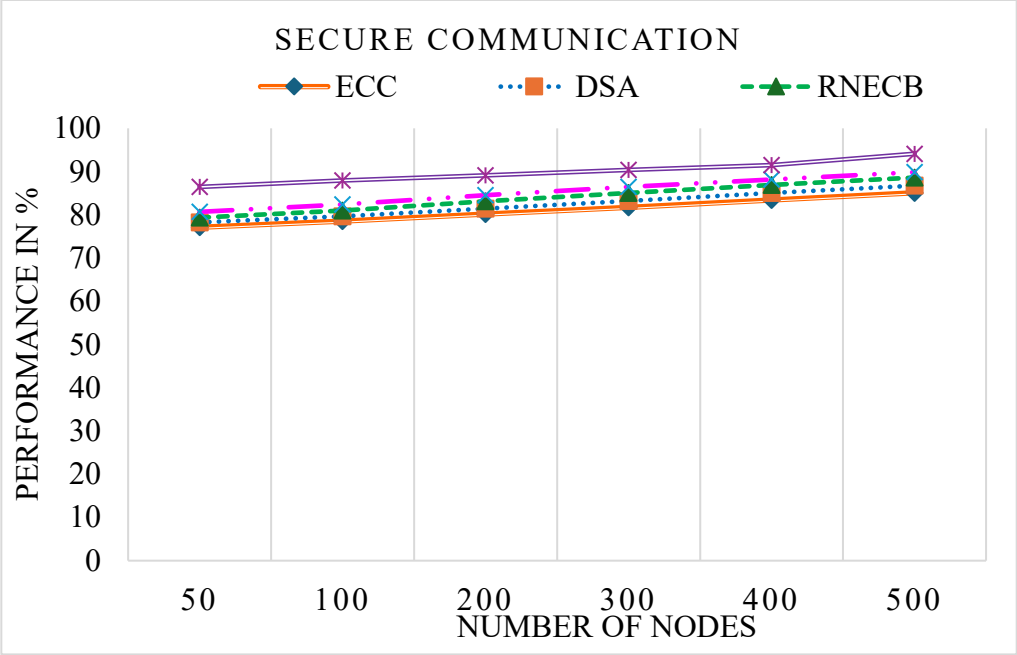

Figure 4. Analysis of Secure Communication

In Figure 4, traditional efficient farming systems are compared with an efficient farming system using blockchain. As the number of IoT nodes increases from 50 to 500, the performance of secure communication gradually improves. The QRKVA method achieves a very high level of secure communication, 94.12%, by combining blockchain verification and encrypted data transmission. Also, for the QRKVA technique and the other techniques (ECC, DSA, RNECB, and SHA-256), the respective security efficiency values are 85.09%, 86.74%, 88.62%, and 89.85% in the performance analysis.

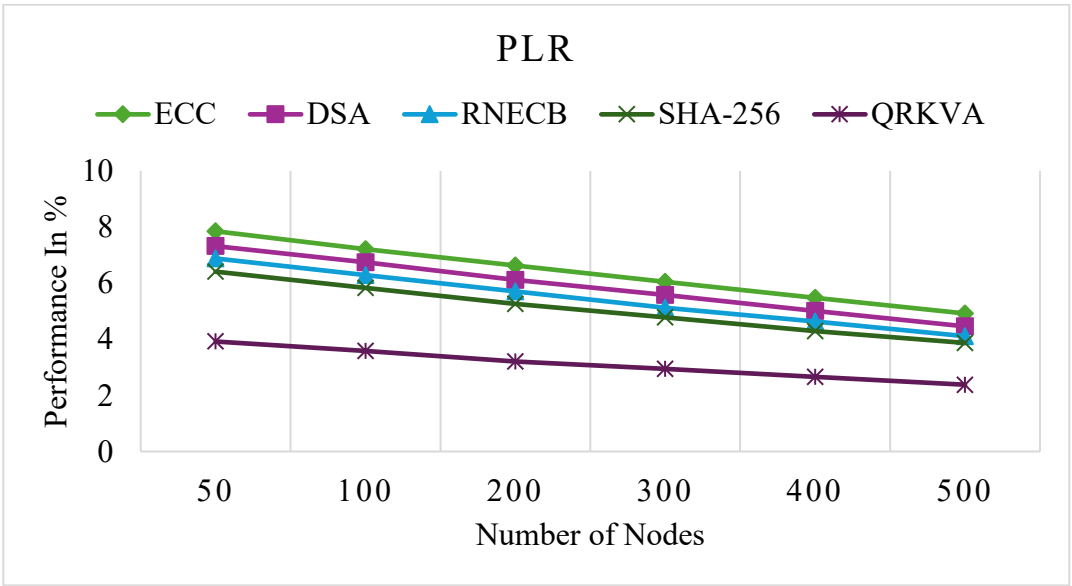

Figure 5. Analysis of PLR

Figure 5 present a comparison between efficient farming with blockchain and traditional efficient farming as the number of IoT nodes increases from 50 to 500, including PLR performance. The QRKVA method achieves a very high PLR of 2.38% by combining blockchain verification with encrypted data transmission. Similarly, the QRKVA

technique, compared with the other techniques (ECC, DSA, RNECB, and SHA－256), has the respective PLR values of (4.92%, 4.46%, 4.11%, and 3.87%) in the performance analysis.

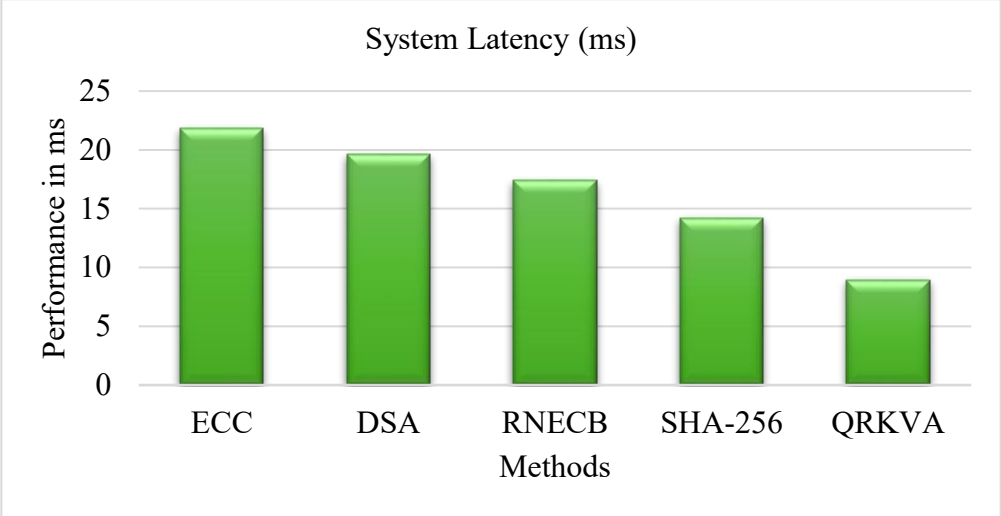

Figure 6. Analysis of Low System Latency

Figure 6 compare efficient farming with blockchain and conventional efficient farming as the number of IoT nodes increased from 50 to 500, including Low System Latency performance. The QRKVA method has a very high PLR of 8.9 ms by integrating blockchain verifications into encrypted data transmissions. Likewise, the QRKVA approach, compared with the other approaches (ECC, DSA, RNECB, and SHA-256), has the respective low system latencies of (21.8 ms, 19.6 ms, 17.4 ms, and 14.2 ms) in the performance analysis.

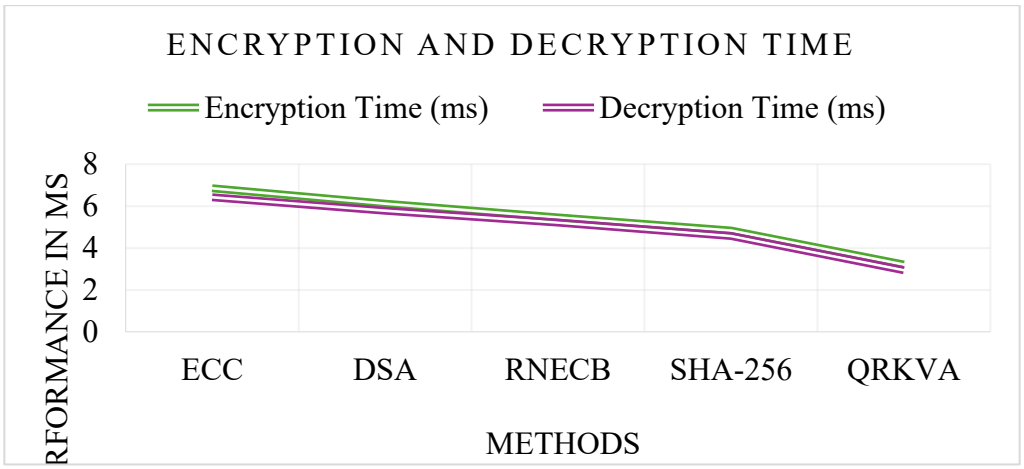

Figure 7. Analysis of Encryption and Decryption Times (ms)

Figure 7 compare blockchain-based efficient farming with traditional efficient farming, including performance in encryption and decryption times (milliseconds) as the number of IoT nodes increases from 50 to 500. The QRKVA method achieves low encryption and decryption time performance (3.21 milliseconds and 2.94 milliseconds, respectively) by combining blockchain verification with encrypted data transmission. Likewise, compared to other techniques (ECC, DSA, RNECB, and SHA-256), the QRKVA technique exhibits lower encryption and decryption times (milliseconds) in the performance analysis.

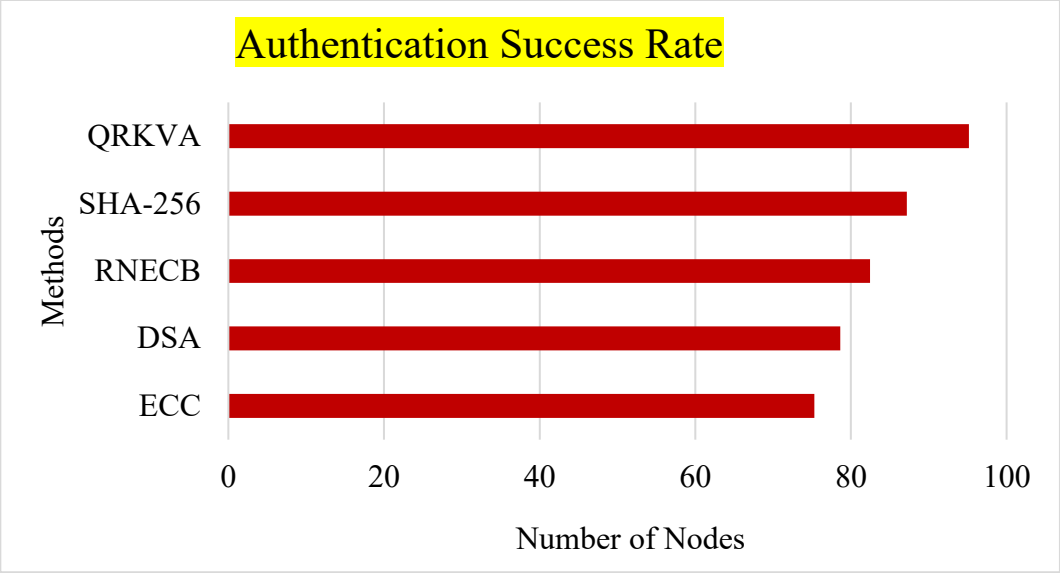

Figure 8. Analysis of Analysis of Authentication Success Rate

Figure 8 compare blockchain-based efficient farming with traditional efficient farming, including authentication success rate performance as the number of IoT nodes increases from 50 to 500. The QRKVA method achieves an authentication success rate performance is (95.16%, respectively) by combining blockchain verification with encrypted data transmission. Similarly, when comparing the QRKVA technique with other techniques (ECC, DSA, RNECB, and SHA-256), the authentication success rates are 75.3%, 78.62%, 82.47%, and 87.18%, respectively.

4.1 Ablation Study

Table 5. Ablation Study of the Proposed QRKVA Framework

Configuration	**Throughput (Mbps)**	**Authentication Reliability (%)**	**Secure Communication (%)**	**Packet Loss Rate (%)**	**System Latency (ms)**	**Encryption Time (ms)**	**Decryption Time (ms)**	**Analysis of Authentication Success Rate (%)**
Baseline IoT System	72.18	77.53	78.24	5.84	24.7	7.92	7.46	76.85
+ HBCA	78.43	82.47	83.18	4.92	20.8	6.84	6.42	81.32
+ BAES-256SA	83.57	86.83	87.56	4.13	16.9	5.31	5.04	85.74
+ PA-CKGA	86.74	89.35	90.41	3.56	13.8	4.42	4.16	89.21
+ RDSA	88.52	91.62	92.76	2.91	10.6	3.78	3.46	92.68
Proposed QRKVA Framework	89.94	93.24	94.12	2.38	8.9	3.21	2.94	95.16

As shown in table 5, the impact of each element in the secure blockchain-assisted IoT framework for smart agriculture is analyzed by the ablation study. The baseline IoT network has the lowest performance in term of all metrics. The adoption of HBCA leads to better throughput and less packet loss by means of secure blockchain blocks formation. The integration of BAES-256SA greatly improves the security of communication, owing to the efficient AES-based scheme, and low computation overhead in both encryption and decryption processes. Additionally, PA-

CKGA enhances Authentication reliability via generating privacy-aware cryptographic keys for access control. To enhance communication security and reduce system delay, RDSA is employed through randomized data shuffling. Besides, by integrating QRKVA, the highest overall security level can also be obtained with a throughput of 89.94 Mbps, authentication reliability of 93.24%, secure communication of 94.12%, packet loss rate of 2.38%, system latency of 8.9 ms, encryption time of 3.21 ms, decryption time of 2.94 ms, and authentication success rate of 95.16%. The results exhibit that each module positively affects system performance and that the integrated framework guarantees the best security, reliability, and efficiency for smart agriculture applications.

5. CONCLUSION

In conclusion, the use of QRKVA was proposed in this paper to enable secure communication and access control, maintain data privacy and security in smart agriculture, and provide a secure blockchain-assisted IoT framework for smart agriculture. The combination of these security features makes this framework highly effective in protecting blockchain operations, ensuring the security of data and transactions, and safeguarding against potential issues caused by future quantum computers. The combination of these elements ensures the safe and reliable data collection, transmission, storage, and retrieval in agricultural operations utilizing IoT-enabled devices. The performance evaluation proves the efficiency of the proposed framework in different security and communication performance measures. The proposed QRKVA framework obtained the highest throughput of 89.94 Mbps, authentication reliability of 93.24%, the security communication efficiency of 94.12%, packet loss rate of 2.38%, system latency of 8.9ms, encryption time of 3.21ms, decryption time of 2.94ms, and an authentication success rate of 95.16%. In addition, the ablation study confirmed the contribution of the various proposed modules towards the overall system performance and security. Based on this, the proposed framework is a secure, reliable, and privacy-preserving smart agriculture solution that can effectively shield agricultural information, guarantee the efficient and reliable operation of agricultural management, and adapt to the complex environment of the next-generation Internet of Things and blockchain technology. Moreover, the implemented threat model in the developed framework is capable of defending against replay attacks, man-in-the-middle attacks, data tampering, unauthorized access and new threats such as those from quantum computing. Moreover, the adoption of NIST standardized post-quantum cryptographic algorithm Dilithium-Kyber further enhances the quantum resistance of the proposed QRKVA framework, and future-proofs it against emerging quantum-computing threats.

5.1 Future Research

Advanced post-quantum cryptographic algorithms and quantum key distribution techniques can be added to future work to further enhance security from emerging quantum computing attacks.

The proposed framework can be further enhanced by incorporating lightweight edge artificial intelligence models with minimal latency for real-time crop monitoring, disease prediction, and intelligent decision-making.

In future, the multi-blockchain or hybrid blockchain design can be explored to enhance scalability, interoperability, and transaction efficiency in large-scale smart agriculture scenarios.

Federated learning techniques that allow for distributed agricultural device collaboration to train a model while maintaining data privacy can be integrated into the framework.

Future research can focus on creating energy-efficient security protocols and optimizations to minimize computational load and power usage in resource-limited IoT devices used in farming.

The system can be integrated with digital twin technology to develop virtual farms and allow for predictive analytics, resource management optimization and intelligent farming management through secure data sharing via the blockchain..

References:

1. Daniel Commey, Sena G. Hounsinou, And Garth V. Crosby, "Securing Blockchain-Based IoT Systems: A Review", VOLUME 12, 2024, Digital Object Identifier 10.1109/ACCESS.2024.3428490.
2. Aliyu, A. A., & Liu, J. (2023). Blockchain-Based Smart Farm Security Framework for the Internet of Things. Sensors (Basel, Switzerland), 23(18), 7992. https://doi.org/10.3390/s23187992
3. Jang, H., Choi, J., Son, S., Kwon, D., & Park, Y. (2024). Provably Secure and Privacy-Preserving Authentication Scheme for IoT-Based Smart Farm Monitoring Environment. Electronics, 14(14), 2783. https://doi.org/10.3390/electronics14142783
4. Kethineni, K., & Gera, P. (2023). Iot-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture. Systems, 11(6), 304. https://doi.org/10.3390/systems11060304.

5. Elkhodr, M. (2025). An AI-Driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain. Future Internet, 17(6), 246. https://doi.org/10.3390/fi17060246.
6. Ali, Iram Asghar, Wajahat Anwaar Bukhari, Muhammad Adnan, Muhammad Ismail Kashif, Afraz Danish, and Ammar Sikander. "Security and privacy in IoT-based Smart Farming: a review." Multimedia Tools and Applications 84, no. 16 (2025): 15971-16031.
7. Senthil kumar, C., Vijay Anand, R. (2024). Security in IOT-Enabled Smart Agriculture Systems. In: Prasad, A., Singh, T.P., Dwivedi Sharma, S. (eds) Communication Technologies and Security Challenges in IoT. Internet of Things. Springer, Singapore. https://doi.org/10.1007/978-981-97-0052-3_14.
8. Alharbi, I.M., Almazmomi, N.K. AI-optimized blockchain security for smart agriculture using post-quantum cryptography and graph neural network-based threat detection. Peer-to-Peer Netw. Appl. 18, 276 (2025). https://doi.org/10.1007/s12083-025-02062-0.
9. Vellimalaipattinam Thiruvenkatasamy, Krishnaprasath, Hayder MA Ghanimi, Sudhakar Sengan, and Meshal Ghalib Alharbi. "An online tool based on the Internet of Things and intelligent blockchain technology for data privacy and security in rural and agricultural development." Scientific Reports 15, no. 1 (2025): 27349.
10. Taji, Khaoula, and Fadoua Ghanimi. "Enhancing security and privacy in smart agriculture: A novel homomorphic signcryption system." Results in Engineering 22 (2024): 102310.
11. M. Xie et al., "Traceability and Identity Protection in Smart Agricultural IoT System Framework Based on Blockchains," in IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 5, pp. 5335-5351, Sept.-Oct. 2025, DOI: 10.1109/TDSC.2025.3565593.
12. Alyahya, S., Khan, W. U., Ahmed, S., Marwat, S. N., & Habib, S. (2021). Cyber Secure Framework for Smart Agriculture: Robust and Tamper-Resistant Authentication Scheme for IoT Devices. Electronics, 11(6), 963. https://doi.org/10.3390/electronics11060963.
13. Itoo, Samiulla, Akber Ali Khan, Musheer Ahmad, and M. Javed Idrisi. "A secure and privacy-preserving lightweight authentication and key exchange algorithm for smart agriculture monitoring system." IEEE Access 11 (2023): 56875-56890.
14. Shreya, Shashi, Kakali Chatterjee, and Ashish Singh. "BFSF: A secure IoT based framework for smart farming using blockchain." Sustainable Computing: Informatics and Systems 40 (2023): 100917.
15. Kaushik, Ila, Nupur Prakash, and Anurag Jain. "An AI-blockchain-assisted smart agriculture framework for enabling secure and efficient data transaction: a hybrid approach." Knowledge and Information Systems 67, no. 11 (2025): 10087-10135.
16. Mahalingam, Nagarajan, and Priyanka Sharma. "An intelligent blockchain technology for securing an IoT-based agriculture monitoring system." Multimedia tools and applications 83, no. 4 (2024): 10297-10320.
17. Vijayaragavan, S., E. PunarSelvam, and N. Kuppurasu. "Decentralized Block Chain Provenance Security System Using Secure Sharable Advanced Encryption Standard for Distributed Agriculture Information Security." NeuroQuantology 20, no. 8 (2022): 6738.
18. Mousavi, Seyyed Keyvan, and Ali Ghaffari. "Data cryptography in the internet of things using the artificial bee colony algorithm in a smart irrigation system." Journal of Information Security and Applications 61 (2021): 102945.
19. Wang, S., Luo, N., Xing, B., Sun, Z., Zhang, H., & Sun, C. (2024). Blockchain-based proxy re-encryption access control method for biological risk privacy protection of agricultural products. Scientific Reports, 14(1), 20048. https://doi.org/10.1038/s41598-024-70533-0
20. Yu, Hui-fang, and Wen-zhuo Mu. "ABE-based postquantum cross-blockchain data exchange approach for smart agriculture." IEEE Transactions on Industrial Informatics 20, no. 10 (2024): 12083-12091.
21. Kee S.N. (2024) Blockchain-Based Authentication and Security for IoT in Smart Agriculture, Insights2Techinfo, pp.1.
22. Kalimuthu, Vinoth Kumar, and Mano Joel PrabuPelavendran. "Blockchain based secure data sharing in precision agriculture: A comprehensive methodology incorporating deep learning and hybrid encryption model." Brazilian Archives of Biology and Technology 67 (2024): e24230858.
23. Zhang, Guofeng, Xiao Chen, Lei Zhang, Bin Feng, Xuchao Guo, Jingyun Ling, and Yanan Zhang. "STAIBT: Blockchain and CP-ABE empowered secure and trusted agricultural IoT blockchain terminal." IJIMAI 7, no. 5 (2022): 66-75.
24. Kiran, Ajmeera, Prasad Mathivanan, Miroslav Mahdal, Kanduri Sairam, Deepak Chauhan, and Vamsidhar Talasila. "Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques." Mathematics 11, no. 9 (2023): 2073.
25. Bhandiwad, Vinita, and Lakshmappa K. Ragha. "Enhancing the security of IOT enabled systems using light weight hybrid cryptography models." Cluster Computing 28, no. 3 (2025): 189.
26. Zhang, G., Chen, X., Feng, B., Guo, X., Hao, X., Ren, H., Dong, C., & Zhang, Y. (2021). BCST-APTS: Blockchain and CP-ABE Empowered Data Supervision, Sharing, and Privacy Protection Scheme for Secure and Trusted Agricultural Product Traceability System. Security and Communication Networks, 2022(1), 2958963. https://doi.org/10.1155/2022/2958963
27. Shaik, Mahaboob Basha, and Yamarthi Narasimha Rao. "Secret Elliptic Curve-Based Bidirectional Gated Unit Assisted Residual Network for Enabling Secure IoT Data Transmission and Classification Using Blockchain." IEEE Access 12 (2024): 174424-174440.

28. Vedula, Kiran Bharadwaj, and Rajesh Arunachalam. "IoT-ethereum blockchain-enabled privacy-preserved framework for pest detection and smart irrigation using adaptive residual Densenet-ASPP with spatial attention." Expert Systems with Applications 313 (2026): 131517.
29. Ahmed, Adeel, Irum Parveen, Saima Abdullah, Israr Ahmad, Nazik Alturki, and Leila Jamel. "Optimized data fusion with scheduled rest periods for enhanced smart agriculture via blockchain integration." Ieee Access 12 (2024): 15171-15193.
30. Bilas Haldar. (2024). An Efficient Multiuser Authentication and Data Transformation Technique for Smart Agriculture Using Cryptography. International Journal of Intelligent Systems and Applications in Engineering, 12(4), 3087–3100. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6802